Vendor Management

Federal Deposit Insurance Corporation
Division of Risk Management Supervision
Atlanta Regional Office

June 18, 2014

Agenda

Introduction

Vendor Management Overview

- Regulatory Expectations
- Board and Management Responsibilities

Framework Guidelines

Contracts

Business Continuity Plans

Common Outsourced Services

- Core Application
- Item Processing
- IT Security
- Audit
- Fraud Analysis
- Website Management
- Card Processing
- Mortgage Servicing

GLBA

- *Oversee Service Provider Arrangements.* Each bank shall:

  1. Exercise appropriate due diligence in selecting its service providers;

  2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and

  3. Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.

Risk Considerations

- Strategic
  - How does this service provider fit into institution’s goals and objectives?
  - Are the Directors involved in the process?
- Transaction/Operations
  - Service-level metrics
  - Disaster recovery
  - Security-related controls
- Credit
  - Cash flow
  - Subcontractors

Risk Considerations (cont.)

- Reputation
  - Interactions not consistent with Institution policies
  - Violations of law and regulations
  - Security breaches disclosing sensitive information
- Country
  - Judicial providence
  - Political considerations
- Compliance
  - Laws, regulations
  - Institution's policies
- Other
  - Interest rate
  - Price
  - Legal
  - Foreign currency

Board and Management Oversight

- Policy Review and Approval
  - Key board function
  - **REVIEW**, not just Approval
- Institute Repeatable Framework
  - Involve various departments of institution
    - Compliance
    - Legal
    - Credit
    - Operations
  - Assign business owner as sponsor of program
- Safeguard Sensitive Information
- Business Continuity Planning
- Reporting
  - Annual report to Board required by GLBA
  - Significant vendors identified

Risk Management Framework

1. Institute Risk Assessments
   - Include key personnel and departments
   - Assign and define risk ranges
   - Identify time and diligence required at each category
2. Identify, Quantify, and Reduce Risk
   - Similar to your enterprise risk assessment
   - Consider qualitative analysis as well
3. Incorporate Reminder Capability
   - Tickler
4. Provide for Ongoing Due Diligence
5. Keep It Simple and Intuitive
   - Flowchart the process

Risk Management Framework (cont.)

6. Use a Similar Process For All Vendors
   - Flexibility is key
7. Maintain Details of Current and Past Reviews
   - Archival
   - Historical
8. Ensure Board Reporting and Involvement

Vendor Checklist

- ✓ Vendor Name and Service
- ✓ Nature of the Service
- ✓ Data
  - ➢ Company data (confidential)
  - ➢ Customer data (sensitive)
  - ➢ Intangible property
  - ➢ Usage
- ✓ Magnitude of Performance Problems
  - ➢ Financial
  - ➢ Reputational
  - ➢ Operational
- ✓ Contractual Details
  - ➢ Date, term, and value of contract

Vendor Checklist (cont.)

- ✓ Interaction frequency with the third party
- ✓ Geographical (global) considerations such as location of third parties and number of physical locations (Business Continuity)
- ✓ Compliance with rules, regulations, law, etc.
- ✓ ID primary relationship owner within the organization
- ✓ Annual spend
- ✓ Risk scoring
- ✓ Audit reports
- ✓ Right-to-audit clause

Contracts (Fees and Costs)

- Legal
- Audit
- Examination
- Equipment
  - Hardware
  - Software
- Fee Calculations
  - Development
  - Programming
  - Conversion
  - Recurring Services
  - Special Requests

Contracts

(Service Performance Clause)

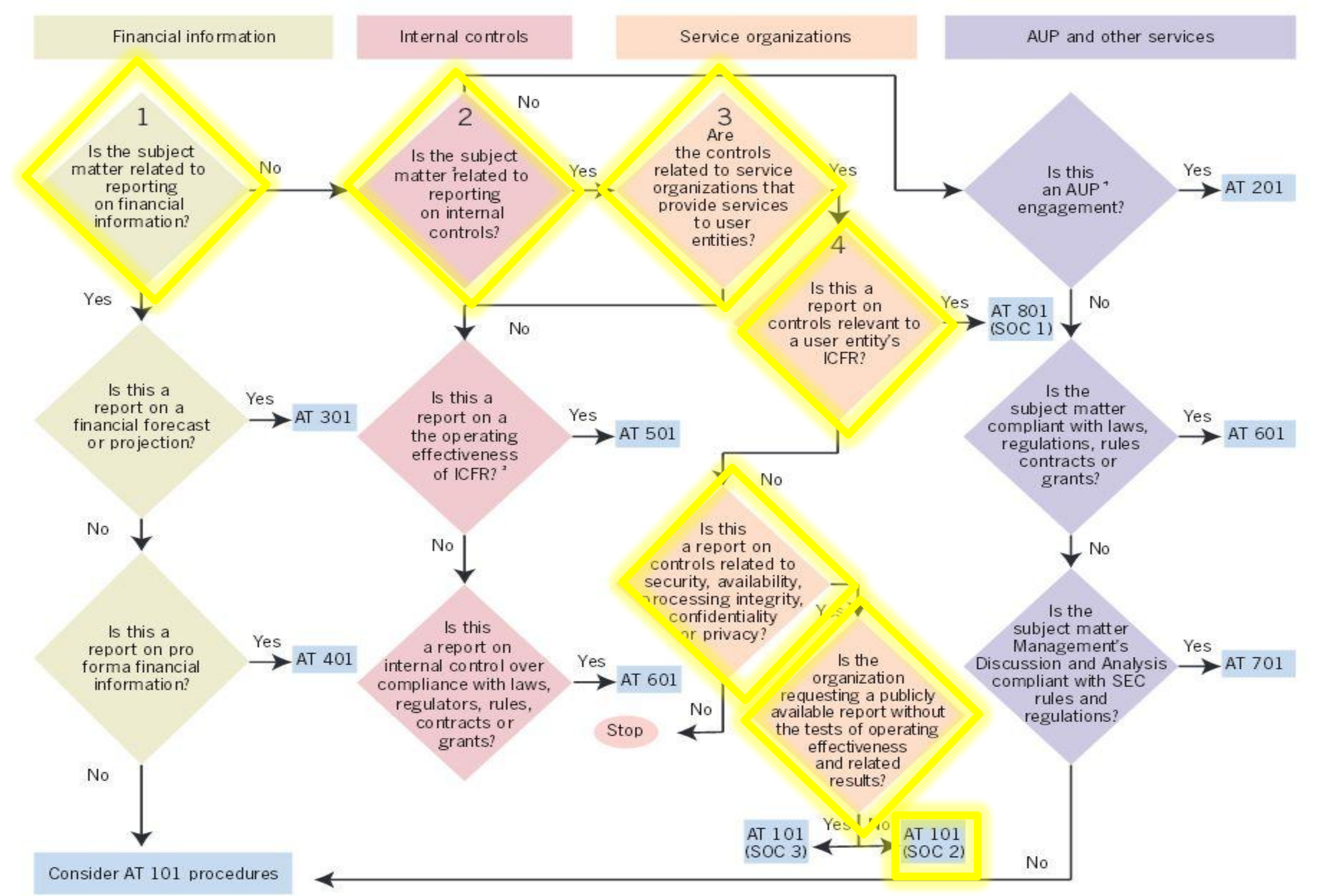
- Response Times
- System Availability
- Data Integrity
- Core Report Availability
  - Frequency
  - Type
  - Quantity
  - Format
  - Archival

- Peripheral Reports
  - Control/Audit
  - Financial
  - Security
  - Business Continuity

SOC Determination

1. Security
2. Availability
3. Processing Integrity
4. Confidentiality
5. Privacy of a System and Its Information

SOC Determination



Financial information

Internal controls

Service organizations

AUP and other services

1 Is the subject matter related to reporting on financial information?

No

Yes

Is this a report on a financial forecast or projection?

Yes

AT 301

No

Is this a report on pro forma financial information?

Yes

AT 401

No

Consider AT 101 procedures

2 Is the subject matter related to reporting on internal controls?

Yes

No

Is this a report on a the operating effectiveness of ICFR? ²

Yes

AT 501

No

Is this a report on internal control over compliance with laws, regulators, rules, contracts or grants?

Yes

AT 601

Stop

3 Are the controls related to service organizations that provide services to user entities?

Yes

No

4 Is this a report on controls relevant to a user entity's ICFR?

Yes

AT 801 (SOC 1)

No

Is this a report on controls related to security, availability, processing integrity, confidentiality or privacy?

Yes

No

Is the organization requesting a publicly available report without the tests of operating effectiveness and related results?

Yes

AT 101 (SOC 3)

No

AT 101 (SOC 2)

Is this an AUP ¹ engagement?

Yes

AT 201

No

Is the subject matter compliant with laws, regulations, rules contracts or grants?

Yes

AT 601

No

Is the subject matter Management's Discussion and Analysis compliant with SEC rules and regulations?

Yes

AT 701

No

² ICFR = Internal Control Over Financial Reporting

¹ AUP = Agreed-upon procedure

Contracts (NPPI)

- **Nonpublic Personally Identifiable Information** data is any list, description, or other grouping of consumers (and publicly available information pertaining to them) derived using any personally identifiable financial information that is not publicly available.

Contracts

(Default and Termination Clause)

- Force Majeure
- Mergers and Acquisitions
- Convenience
- Substantial Increase in Cost
- Repeated Failure to Meet Service Levels
- Failure to Provide Critical Services
- Bankruptcy
- Insolvency

Contracts

(Ownership and License)

- Ownership Rights
  - Source Code Access
  - Intellectual Property
- Use of Institution's Data
  - Data Mining
  - Marketing
- Use of Processing Hardware
- Use of Software
  - Virtualization
  - Operating System
  - Application
  - Updates

Contracts

(Cloud Computing)

- Three Most Important Contract Considerations
  - Data Protection
  - Data Security
  - Jurisdiction
- Security Schedule Recommendations
  - Institution’s data separated from others in Cloud
  - Restrictions on use of data
  - Responses to security breaches
  - Use of security measures such as encryption
  - Access to Vulnerability and Penetration tests
- Natural Concerns
  - Loss of confidentiality (unauthorized disclosure)
  - Loss of integrity (corruption)
  - Loss of availability (deletion)
- End of Contract Concerns
  - Access to data
  - Deletion of data
  - Application
  - Updates

Contracts (Subcontracting)

- Primary Servicer Accountable
  - Must have visibility into subcontractors.
- Define Services, Performance
  - Create metric table.
  - Can be in form of "Dashboard".
  - Periodically review performance.
- Primary Servicer's Due Diligence Process
  - How does the primary service provider assess contractors?
- Approval Process for Change
  - Institution notified?
  - Institution given choices?
- Foreign Firms

Contracts (Insurance)

- ❑ Who is responsible for errors or omissions?
- ❑ What about negligence?
- ❑ Will the service provider cover any losses of revenue?

BCP Vendor Checklist

- ❑ Ensure a disaster recovery and business continuity plan exists and is included in the contract;
- ❑ Assess the adequacy and effectiveness of disaster recovery and business continuity plans and its alignment to your own plan;
- ❑ Document the roles and responsibilities for maintaining and testing the service provider's business continuity and contingency plans;
- ❑ Test the service provider's business continuity and contingency plans on a periodic basis; and,
- ❑ Maintain an exit strategy.

Customer Notice

- Standard for Providing Notice
- Defining Customer Information
- Affected Customers
- Content of Customer Notice
- Delivery of Customer Notice

Thank You!

Richard Snitzer

IT Examination Specialist

FDIC Atlanta Regional Office

678.916.2224

rsnitzer@FDIC.GOV

Sources and References

FFIEC Supplement to Authentication in an Internet Banking Environment (FIL-50-2011)

FFIEC Retail Payment Systems Handbook (FIL-6-2010)
Special Alert SA-147-2009: *Fraudulent Electronic Funds Transfers* (August 2009)

FFIEC Guidance on Risk Management of Remote Deposit Capture (FIL-4-2009)

Identity Theft Red Flags, Address Discrepancies, and Change of Address Regulations Examination Procedures (FIL-105-2008)

FFIEC Guidance: Authentication in an Internet Banking Environment (FIL-103-2005)

Sources and References (cont.)

Payment Processor Relationships-Revised Guidance (FIL-3-2012)

Guidance for Managing Third-Party Risk (FIL-44-2008)

FDIC Supervisory Insights Journal (Quarterly)

National Institute of Standards & Technology (NIST)

Trade Associations (ABA, BITS)

Part 364-B, FDIC Rules and Regulations

PCI Security Standards Council

US CERT

Sources and References (cont.)

Kitten, T. (2013, July 29). New Details on Global, Heartland Breaches. Http://www.bankinfosecurity.com. Retrieved May 29, 2014. http://www.bankinfosecurity.com/card-fraud-case-sheds-light-on-breaches-a-5946.

Vijayan, J. (2010, May 10). Heartland breach expenses pegged at $140M – so far. Http://www.computerworld.com. Retrieved May 29, 2014. http://www.computerworld.com/s/article/9176507/Heartland_breach_expenses_pegged_at_140M_so_far.

Bradshaw, S., Millard, C., Walden, I. (2010, September 1). Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. https://hq.ssrn.com/. Retrieved May 28, 2014. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374.